SPYWOLF

Security Audit Report

Completed on

January 18, 2023

OVERVIEW

This audit has been prepared for **Schipperke Inu** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

SCHIPPERKE INU

PROJECT DESCRIPTION

According to their website:

Schipperke Inu $SCHIPS is an innovative new ERC-20 meme token on the Ethereum Network that gives out $BONE rewards every 8 hours to those who hold! Curious, lively, and intense but mischievous, this little black dog is a robust, long-lived companion for whom there is never a dull moment with 2% Shiba $BONE rewards.

Release Date: January 17th, 2023

Category: Meme token

CONTRACT INFO

Token Name Schipperke Inu	Symbol SCHIPS
Contract Address 0x98aDA56008FB2998E14C9f37818e663f689e2252	
Network Ethereum	Language Solidity
Deployment Date Jan 17, 2022	Verified? Yes
Total Supply 1,000,000,000,000	Status Launched

TAXES

Buy Tax	Sell Tax
6%	7%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of January 18, 2022)

Status:
Launched!

Liquidity

Uniswap V2:
24.6 WETH

Burn

No burnt tokens

MaxTxAmount
200,000,000,000

DEX
Uniswap

LP Address(es)

Uniswap:
0x024744aA34F8410B48623B124Dce50e7b965E3B1

99% locked in Unicrypt - unlocks at 18/04/2023
https://app.unicrypt.network/amm/uni-v2/pair/0x024744aA34F8410B48623B124Dce50e7b965E3B1

TOKEN TRANSFERS STATS

Transfer Count	695
Uniq Senders	86
Uniq Receivers	182
Total Amount	3173060039452.0903 SCHIPS
Median Transfer Amount	934520799.4536414 SCHIPS
Average Transfer Amount	4565554013.60013 SCHIPS
First transfer date	2023-01-17
Last transfer date	2023-01-18
Days token transferred	2

SMART CONTRACT STATS

Calls Count	1299
External calls	180
Internal calls	1119
Transactions count	502
Uniq Callers	154
Days contract called	2
Last transaction time	2023-01-18 15:49:47 UTC
Created	2023-01-17 15:03:23 UTC
Create TX	0x87928ebe7d1a1dbd96b29b77f60fd7f1a72babfb40340cf32f07dce5659f220e
Creator	0x81b627401f7e8a557405080446fcb2db72e5d242

FEATURED WALLETS

Owner address	0x81B627401F7E8A557405080446fCB2Db72e5d242
Dev receiver	Same as owner
Marketing receiver	0x3FcC39Fce78Cec54cC4ee9F654480dC16cB494f1
Liquidity receiver	Same as owner
Liquidity pair	0x024744aA34F8410B48623B124Dce50e7b965E3B1 99% locked in Unicrypt - unlocks at 18/04/2023 https://app.unicrypt.network/amm/uni-v2/pair/0x024744aA34F8410B48623B124Dce50e7b965E3B1

TOP 3 UNLOCKED WALLETS

1 2% 0x295fd114d4413815ce897e2111122329a38ab4df

0xbdb7b80e671774989def74c3a1227f95cea83db4 1.32% 2

3 1.30% 0x6ba8894d245b7a321577ac9a2a4ea702695bea35

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium Risk

Owner can blacklist addresses - making it impossible to sell (applying 99% fees to blacklisted address).

```
function setisBot(address _address, bool _enabled) external onlyOwner {
    require(_address != address(pair) && _address != address(router) && _address != address(this),
    "Ineligible Address");
    isBot[_address] = _enabled;
}
```

⚠ Low Risk

Owner can set buy/sell fees up to 20%.
Combined buy+sell = 40%.

```
function setStructure(uint256 _liquidity, uint256 _marketing, uint256 _burn, uint256 _rewards,
uint256 _development, uint256 _total, uint256 _sell, uint256 _trans) external onlyOwner {
    liquidityFee = _liquidity;
    marketingFee = _marketing;
    burnFee = _burn;
    rewardsFee = _rewards;
    developmentFee = _development;
    totalFee = _total;
    sellFee = _sell;
    transferFee = _trans;
    require(totalFee <= denominator.div(5) && sellFee <= denominator.div(5)
    && transferFee <= denominator.div(5), "totalFee and sellFee cannot be more than 20%");
}
```

Informational

Owner can withdraw any tokens from the contract.

```
function rescueERC20(address _address, uint256 _amount) external onlyOwner {
    IERC20(_address).transfer(msg.sender, _amount);
}
```

Owner can exclude address from dividends.

```
function setisDividendExempt(address holder, bool exempt) external onlyOwner {
    isDividendExempt[holder] = exempt;
    if(exempt){setShare(holder, 0);}
    else{setShare(holder, balanceOf(holder)); }
}
```

Owner can set max transaction limit but cannot lower it than 0.5% of total supply.

```
function setParameters(uint256 _buy, uint256 _trans, uint256 _wallet) external onlyOwner {
    uint256 newTx = (totalSupply() * _buy) / 10000;
    uint256 newTransfer = (totalSupply() * _trans) / 10000;
    uint256 newWallet = (totalSupply() * _wallet) / 10000;
    _maxTxAmount = newTx;
    _maxSellAmount = newTransfer;
    _maxWalletToken = newWallet;
    uint256 limit = totalSupply().mul(5).div(1000);
    require(newTx >= limit && newTransfer >= limit && newWallet >= limit,
    "Max TXs and Max Wallet cannot be less than .5%");
}
```

Informational

Owner can withdraw any tokens from the contract.

```
function setisExempt(address _address, bool _enabled) external onlyOwner {isFeeExempt[_address] = _enabled;}

function _transfer(address sender, address recipient, uint256 amount) private {
    ..............
    checkMaxWallet(sender, recipient, amount);
    checkTxLimit(sender, recipient, amount);
    ..............
    }

function checkTxLimit(address sender, address recipient, uint256 amount) internal view {
    if(sender != pair)
    {require(amount <= _maxSellAmount || isFeeExempt[sender] || isFeeExempt[recipient], "TX Limit Exceeded");}
    require(amount <= _maxTxAmount || isFeeExempt[sender] || isFeeExempt[recipient], "TX Limit Exceeded");
}

 function checkMaxWallet(address sender, address recipient, uint256 amount) internal view {
    if(!isFeeExempt[sender] && !isFeeExempt[recipient] && recipient != address(pair) && recipient != address(DEAD)){
    require((_balances[recipient].add(amount)) <= _maxWalletToken, "Exceeds maximum wallet amount.");}
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

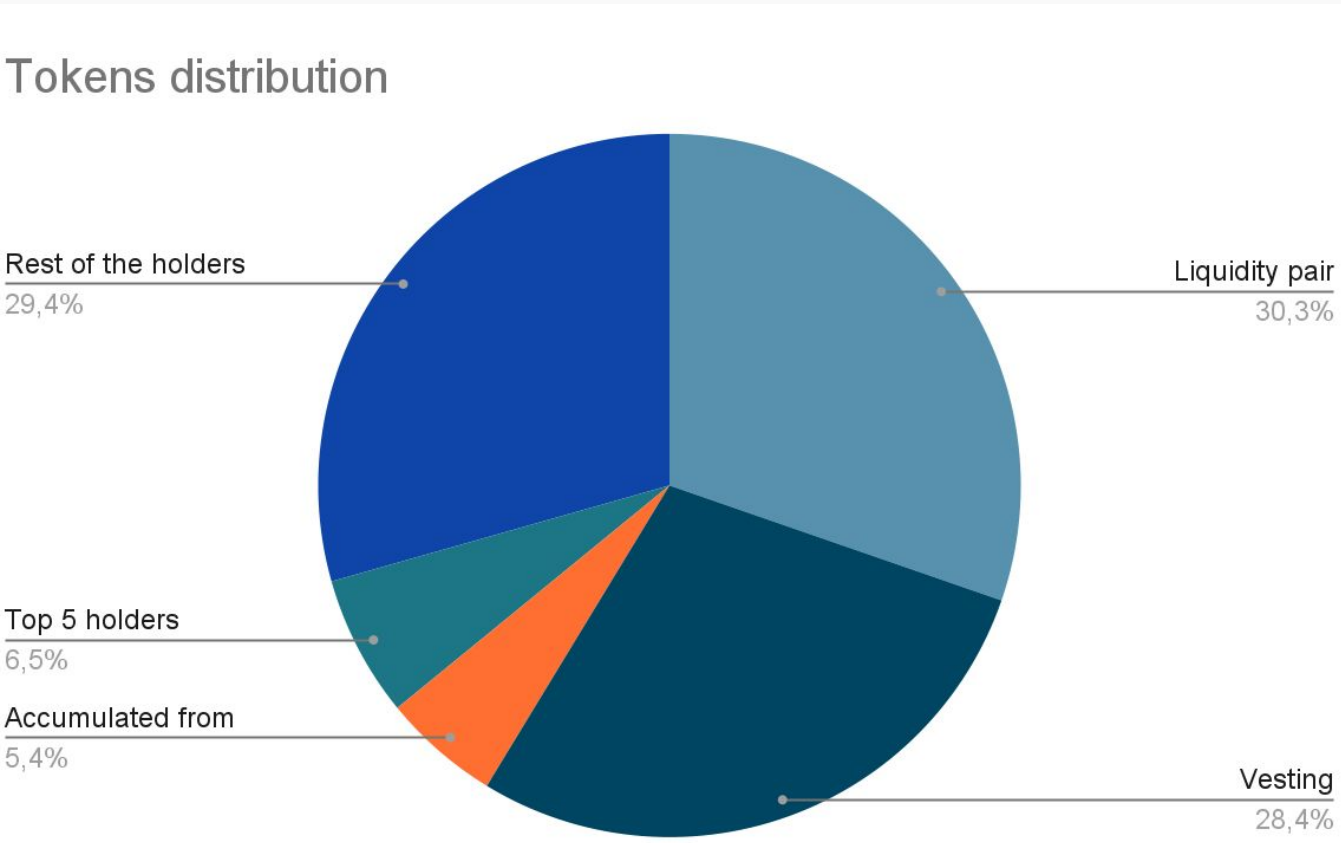
Schipperke Inu

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner can set a transaction limit, but can’t lower it than 0.5% of total supply
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

Tokens distribution according to Etherscan:

- 30.3% - Liquidity pair
- 28.4% - Unicrypt Vesting*
- 5.43% - Accumulated from taxes in the contract
- 6.5% - Top 5 holders
- 29.4% - Rest of the holders



* For more information regarding vesting periods, visit the Unicrypt page below:
https://app.unicrypt.network/amm/uni-v2/token/0x98aDA56008FB2998E14C9f37818e663f689e2252

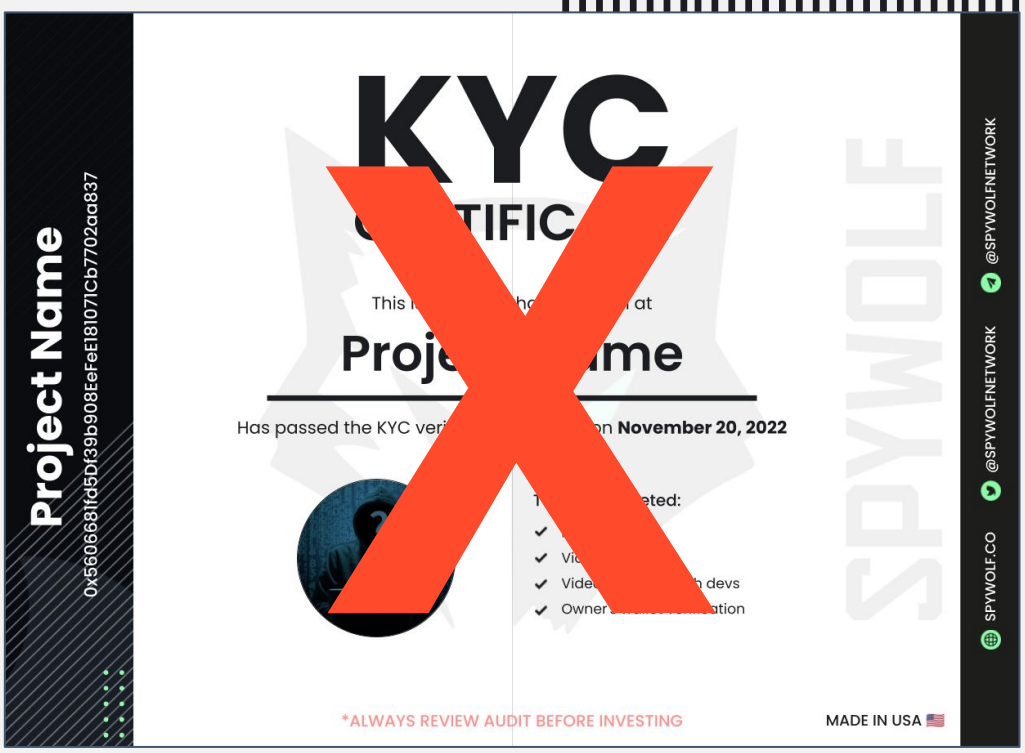
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://www.schipperkeinu.com

Domain Registry
https://www.wix.com

Domain Expiration
Expires on 2024-01-05

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design with appropriate color scheme and nice graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set with time frames.

Mobile-friendly?
Yes

schipperkeinu.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active with organic members

Twitter

@Schipperkelnu

- 113 followers
- Posts frequently
- Active

Discord

- Not available

Telegram

@SchipperkelnuCommunity

- 82 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.